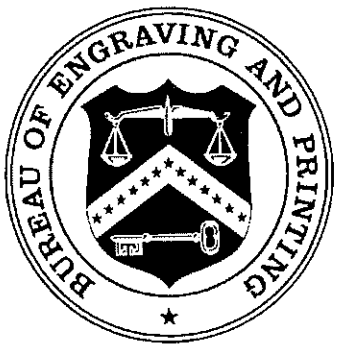

Department of the Treasury
Bureau of Engraving and Printing

Privacy Impact Assessment (PIA) Procedures

MAIL ORDER SALES CUSTOMER FILES

Office of Critical Infrastructure
and Information Technology Security
January 2004

Introduction

The Bureau of Engraving and Printing is required to protect the privacy to which employees and the public are entitled by law. The Privacy Act Assessment (PIA) provides a means for integrating the consideration of privacy issues into the development of information systems. Section I of this document provides background information on the PIA, steps for completing the PIA process, and an overview of privacy issues in information systems. Section II is the Privacy Impact Assessment tool. Section III provides a privacy impact analysis. Section IV identifies basic privacy requirements to be addressed during the systems development lifecycle.

Section I

Purpose

The Privacy Impact Assessment assists in identifying and addressing information privacy when planning, developing, implementing, and operating information systems. The assessment process gathers information for use in identifying and evaluating compliance with applicable statutory requirements. These requirements are drawn from the Privacy Act; E-Government Act; Government Paperwork Reduction Act; Freedom of Information Act; and Office of Management and Budget (OMB) Circulars A-130: Management of Federal Information Resources, A-123: Management Accountability, and A-11: Preparation, Submission and Execution of the Budget.

Goals accomplished in completing a PIA include:

- Providing senior management with the tools to make informed policy and system design or procurement decisions based on an understanding of privacy risk, and of options available for mitigating that risk;

- Ensuring accountability for privacy issues with the system project manager and system owner;

- Ensuring a consistent format and structured process for analyzing both technical and legal compliance with applicable privacy law and regulation, as well as accepted privacy policy; and

- Providing basic documentation on the flow of personal information within Bureau systems for use and review by policy and program staff, systems analysts, and security analysts.

What is personal information?

Personal information is information about an identifiable individual that may include but is not limited to:

- Information relating to race, national or ethnic origin, religion, age, marital or family status;

- Information relating to education, medical, psychiatric, psychological, criminal, financial or employment history;

- Any identifying number symbol, or other particular assigned to the individual; and

- Name, address, telephone, number, finger or voice prints, or a photograph.

When is a PIA required?

The Bureau requires that Privacy Act Assessments be completed for all Bureau information systems. PIAs are also required to be performed and updated as necessary when a system change creates new privacy risks. In addition, OMB requires that a PIA be submitted with Exhibit 300 for all new or significantly altered information technology investments administering information in an identifiable form collected from the public. The E-Government Act also requires publication of the PIA for websites available to the public, and websites or information systems operated by a contractor on behalf of the Bureau for the purpose of interacting with the public.

Suppose the system I am evaluating has no personal information in it?

If the system being evaluated does not contain any personal information identifiable to an individual, complete Section II A. System Information, Section III Privacy Impact Analysis, and Section IV System Development Lifecycle Privacy Requirements Worksheet.

Who completes the PIA?

Since, privacy must be considered when requirements are being analyzed and decisions being made about data usage and system design or procurement, both the system owner, and the system analyst or developer work together to complete the PIA. Once the assessment is completed, the Chief, Office of Administrative Services reviews the PIA to determine privacy risks, and the Manager, IT Security Division reviews the PIA, assesses risks, and recommends risk mitigation strategies.

When must a PIA be completed?

Privacy requirements must be identified and addressed early in the process of planning, developing/procuring, implementing, and modifying information systems that contain personal information (this applies not only to Privacy Act systems of records where personal information is retrieved by the subject's name or identifier, but to any system that contains personal information)

Process for Identifying and Addressing Privacy and Security Issues

The Privacy Impact Assessment is designed to gather information necessary to identify privacy and security risks. Results of the PIA are then evaluated to identify basic privacy and security issues and requirements that are addressed during the systems development lifecycle process.

Step	Participants	Procedure
Conduct Privacy Impact Assessment		
1	System Owner, and System Developer/Analyst	Obtain a copy of the PIA. Office of Administrative Services, _____ and the Office of Critical Infrastructure, Information Technology Security Division are available for consultation on privacy, security, records, and Freedom of Information Act issues.
2	System Owner, and System Developer/Analyst	Complete the PIA.
Evaluate PIA, Identify Risks and Requirements		
3	Chief, Office of Administrative Services	Review the PIA to identify privacy risks and get clarification from the system owner and developer/analyst as needed.
4	Manager, IT Security Division	Review the PIA, assess privacy risks and identify security risks, and recommend mitigation strategies. Prepare risk assessment to document risks and mitigation strategies.
	Chief, Office of Administrative Services; Manager, IT Security Division; System Owner; System Developer/Analyst	Complete Privacy Impact Analysis.
	Chief, Office of Administrative Services; Manager, IT Security Division; System Owner; System Developer/Analyst	Complete Systems Development Privacy Requirements Worksheet
Address Privacy and Security Issues		
5	System Owner; System	Reach agreement on design and implementation

	Developer/Analyst; Privacy Officer; Manager, IT Security Division	requirements to mitigate privacy and security risks.
6	System Owner, and System Developer/Analyst	Incorporate the agreed upon requirements. Update the PIA to reflect elements not identified at the initial concept stage, new information collection, or to address choices made in designing the system or information collection as a result of the analysis

Definitions

Accuracy. Within sufficient tolerance for error to assure the quality of the record in terms of making a determination.

Bureau Information System. An IT system that is owned, leased, or operated by the Bureau; or operated by a contractor or another government agency on behalf of the Bureau.

Completeness. All elements necessary for making a determination are present before a determination is made.

Individual. A citizen of the United States or an alien lawfully admitted for permanent residence.

Record. Any item, collection, or grouping of information about an individual that is maintained by an agency, including but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as finger or voice print or a photograph.

Relevance. Limitation to only those elements of information which clearly bear on the determination(s) for which the records are intended.

System of Records. A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

System Owner/Manager. This is the official responsible for this system who will ensure the implementation of legal information resources management requirements (privacy, security, Freedom of Information Act, records, data administration). For a system of records, this is the system manager documented in the SOR notice.

Privacy Issues in Information Systems

OMB Circular A-130: Management of Federal Information Resources requires that:

- "The individual's right to privacy must be protected in Federal Government information activities involving personal information."

And that agencies will:

- "Consider the effects of their actions on the privacy rights of individuals, and ensure that appropriate legal and technical safeguards are implemented;

The Privacy Act of 1974 5 U.S.C. 552a As Amended requires Federal Agencies to protect personally identifiable information. It states specifically:

"Each Agency that maintains a system of records shall—"

- "maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive order of the President;"

- "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's right's benefits, and privileges under Federal programs;"

- "inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual-" of the authority which authorizes the solicitation of the information and whether disclosure of the information is mandatory or voluntary, principle purpose and routine uses of the information being collected from them, and any effects upon the individual of not providing all or part of the requested information;"

- "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination;"

- "establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance;"

- "establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to the individual on whom the information is maintained;"

OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 dated September 26, 2002 states that:

- Agencies must consider the information lifecycle (i.e. collection, use, retention, processing, disclosure and destruction) in evaluating how information handing practices at each stage may affect individual's privacy. To be comprehensive and meaningful, privacy impact assessments require collaboration by program experts as well as experts in the areas of information technology, IT security, records management, and privacy.

OMB Memorandum M-99-05, Instructions on Complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records" dated January 7, 1999 states that:

- "Systems of records should not be inappropriately combined. Groups of records which have different purposes, routine uses, or security requirements, or which are regularly accessed by different members of the agency staff, should be maintained and managed as separate systems of records to avoid lapses in security. Therefore, agencies shall ensure that their system of records do not inappropriately combine groups of records which should be segregated. This ensures, for example, that routine uses which are appropriate for a certain group of records do not also apply to other groups of records simply because they have been placed together in a common system of records"

Section II

Bureau of Engraving and Printing Privacy Impact Assessment

A. System Information
1. What is the system name? **Mail Order Sales Customer Files (Systems Applications and Products).**
2. What is the purpose and intended use of this system? **The purpose and intended use of this system is to process sales orders and maintain an inventory of products sold and in stock. The system also maintains a data base of customer notification information. It enables the search of customer orders and transmits credit card information to financial institutions for approval or disapproval.**

3. Does this system contain any personal information about individuals? (If no, a PIA is not required. Skip to Section III.)

Yes

4. What legal authority authorizes the purchase or development of this system/application? (List the statutory provisions or Executive Orders that authorize the maintenance of this information to meet an official program mission or goal)

5 U.S.C. 301

5. For new systems, describe how privacy is addressed in documentation related to system development, including as warranted and appropriate, statement of need, functional requirements analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and especially, the initial risk assessment?

This is an existing system.

B. Data in the System

1. What categories of individuals are covered in the system? (e.g. employee, contractor, public)

Public

2. What are the sources of information in the system?

a. Is the information collected directly from the individual or is it taken from another source? If information is not collected directly from the individual, describe the source of the information.

Information is collected directly from the individual.

b. What Federal agencies provide data for use in the system?

Not applicable.

c. What State and Local agencies provide data for use in the system

Not applicable.

d. What other third parties will data be collected from?

Not applicable.

e. **What information will be collected from the employee and the public?** (Be as specific as possible. List personal information collected from the public such as social security number, address, credit card number, telephone number. Employee information may include badge number, user identifier, telephone number, social security number, and health information.)

Mail order customer's name, address, telephone number, company name, credit card number and expiration date; history of customer sales; and inventory data.

3. How does the Bureau ensure that data is sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations about any individual?

a. **How is data accuracy ensured?**

At the time of order, data is verified with the customer, and credit card information is verified with the credit card company to ensure accuracy.

b. **How will data be checked for completeness?**

Once data is entered, mail order information is edited through the use of a mail order edit list.

c. **Is the data current? What steps or procedures are taken to ensure the data is not out-of-date? The data is current. Files on customers who have not purchased any products are kept for two years, after which they are taken out of the active system and placed in a separate storage file. This file generates two additional mailings after which they are purged from the system.**

d. **Are the data elements described in detail and documented? If yes, what is the name of the document?**

Yes, they are. The document name is Create Sales Order Screen.

e. **How will data collected from sources other than BEP records be verified for accuracy?**

Not applicable. BEP's records are the only sources of information.

4. Describe what opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of information (other than required or authorized uses), and how individuals can grant consent.)

Information is voluntary. When customers place an order they must provide specific information to complete the order. They are given the option at that time of being added to the BEP mailing list. If they chose not to join the mailing list their data will be purged after the sales order is completed.

C. Attributes of the Data
1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed? Yes
2. Will the system derive new data or create previously unavailable data about an individual through the aggregation of information collected? (if no, skip to D.3) No **a. Will the new data be placed in the individual's record?** **b. Can the system make determinations about employees or the public that would not be possible without the new data?** **c. How will the new data be verified for relevance and accuracy?**
3. Do the records in this system share the same purpose, routine use, and security requirements? **a. If the data is being consolidated, what technical, management, and operational controls are in place to protect the data from unauthorized access or use? Explain** **b. If processes are being consolidated, are the proper technical, management, and operational controls remaining in place to protect the data and prevent unauthorized access? Explain.**
8. How will the data be retrieved? Can a personal identifier be used to retrieve data? Are personal identifiers used to retrieve data on a routine, occasional, or ad-hoc basis? If yes,

explain and list the identifiers what will be used to retrieve information on the individual.
9. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

D. Maintenance of Administrative Controls
1. If the system is hosted and/or used at more that one site, how will consistent use of the system and data be maintained at all sites?
2. What are the retention periods of the data in this system?
3. What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented? Files on customers who have not purchased any products are kept for two years, after which they are taken out of the active system and placed in a separate storage file. This file generates two additional mailings after which they are purged from the system. The procedures are documented in 70 FR 43508, 43517, July 27, 2005.
4. Is the system using technologies in ways that the BEP has not previously employed (e.g. monitoring software, Caller ID)? If yes, how does the use of this technology affect public/employee privacy? No
5. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain. No a. What kinds of information are collected as a function of the monitoring of individuals? b. What controls will be used to prevent unauthorized monitoring?
6. Under which Privacy Act systems of records notice does the system operate? Provide name and number. Mail Order Sales Customer Files – Treasury/BEP .045
7. If the system is being modified, will the Privacy Act system of records notice require amendment of revision? Explain. No

E. Access to Data
1. Who will have access to the data in the system? (e.g. contractors, users, managers, system administrators, developers, other) Access is limited to those individuals (i.e., BEP managers and contractors) who process orders or maintain the computer system.
2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Access to electronic records is by password for the individuals identified in E.1.
3. Will users have access to all data on the system or will the user's access be restricted? Explain. Users will have access to all data on the system.
4. What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by those having access? (List procedures and training materials) Controls are in place to prevent misuse. Contractors and BEP employees with access to the system are covered by the BEP Standards of Conduct and are trained and supervised to prevent the theft of personal information. In addition, Contractors must conform to Section H.9 of the Statement of Work for BEP Contract TEP-05-0020 which provides the proper procedure for the disclosure of information. All credit card activity is verified and monitored for accuracy against Mellon Bank Credit Card Statements and Treasury's Cashlink. All credits are approved by BEP management. If there is suspicious credit card activity, the cardholder would protest the charge through the chargeback process. Mellon Bank would submit a chargeback request and BEP would research the particular charge in question.
5. Are contractors involved with the design and development of the system and/or will they be involved with the maintenance of the system? (If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed? Yes. Contractors assist with the maintenance of the system. All contracts address privacy issues when contractors are used by IT.
6. Do other systems share data or have access to the data in the system? If yes, explain. Yes. Credit card numbers and other personal data used as identification is shared with financial institutions for the purpose of receiving and transferring funds obtained by the Bureau in exchange for sales products.

7. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface? The Chief of the Office of External Relations is responsible.
8. Will other agencies share or have access to the data in this system? If yes list agencies. No
9. How will the data be used by the other agency? Not applicable.
10. Who is responsible for assuring proper use of the data? The Bureau of Engraving and Printing's Chief of the Office of External Relations is responsible for assuring the proper use of the data.

Section III

Privacy Impact Analysis

System of Records Identification
1. Is a system of records being created under the Privacy Act, 5 U.S.C. 552a. If no, skip questions 2 through 4. Yes. This is an existing system of records, Treasury/BEP .045 – Mail Order Sales Customer Files.
2. Have privacy and IT risk assessments been conducted that consider: the alternatives to collection and handling as designed, and the appropriate measures to mitigate risks identified for each alternative? Risk assessments were conducted as part of the Certification and Accreditation of the system. Appropriate controls to mitigate risk are developed and implemented before a system goes on line.

3. What impact will this system have on an individual's privacy? (Consider the consequences of collection and flow of information and identify and evaluate threats to individual's privacy.) **The impact is considered moderate based upon OMB M-06-16 guidance that credit card numbers represent the need for a higher level of protection.**
4. As a result of the PIA what choices have been made regarding the IT system of collection of information? Have adequate measures been designed and implemented to mitigate risk? What is the rationale for the final design choice or business process? **None. The system was set up prior to the introduction of PIAs. This is a COTS system developed to provide secure financial transactions. The system was adopted to replace a non-compliant Wang system in advance of Y2K. See answer 2 above.**

Section IV

System Development Lifecycle Privacy Requirements Worksheet

A. Contact Information
1. Person who completed the Privacy Impact Assessment document Name: Edward J. Sheehan Title: Public Affairs Specialist Organization: Office of External Relations Phone number: (202) 874-3913
2. System Owner Name: Dawn A. Haley Title: Chief, Office of External Relations Organization: Office of External Relations Phone number: (202) 874-3545
3. IT Security Reviewer Name: Harry Singh Title: Manager, IT Security Organization: IT Security Phone number: (202) 874-0003
4. Bureau Privacy Reviewer Name: Patricia A. Warden Title: Disclosure Officer Organization: Office of Administrative Services Phone number: (202) 874-2582

Privacy Impact Assessment Summary		
System Category (check all categories that apply)		**Requirement**
X	System of Records	Publish System of Records Notice
	Website available to the public	Publish Privacy Impact Assessment
	Website or information system operated by a contractor on behalf of the Bureau for the purpose of interacting with the public	Publish Privacy Impact Assessment
X	New or significantly altered information technology investment administering information in an identifiable form collected from or about members of the	Conduct Privacy Impact Assessment

	public	
	New or significantly altered information technology investment administering information in an identifiable form collected from or about Bureau employees	
	Contains medical information	Determine if system is subject to HIPAA
	Other	
	None of the above	Privacy Impact Assessment not required

Privacy Impact Assessment Approval

Approval of Privacy Impact Assessment accuracy and completeness.

System Owner: Dawn Haley (Signature) 9-18-06 (Date)

Name: Dawn A. Haley
Title: Chief, Office of External Relations

Approval of IT System Risk Assessment

Manager, IT Security Division: (Signature) 09-25-06 (Date)

Name: Harry Singh
Title: Manager, IT Security

Approval of Privacy Assessment and Resulting System Category

Privacy Act Officer: (Signature) 9/27/06 (Date)

Name: Patricia A. Warden
Title: Chief, Office of Administrative Services